ИСПОЛЬЗОВАНИЕ МЕТОДОВ ФУНКЦИОНАЛЬНОГО ДИАГНОСТИРОВАНИЯ ДЛЯ ОБНАРУЖЕНИЯ ОШИБОК ШИФРОВАНИЯ В КРИПТОГРАФИЧЕСКИХ СИСТЕМАХ

Караман Д.Г.
Национальный технический университет «Харьковский политехнический институт», г. Харьков

Общепринятой практикой для защиты передаваемой или хранимой информации стало использование различных криптографических средств. Благодаря открытости и доступности описания, для большинства наиболее часто используемых симметричных алгоритмов шифрования была доказана их стойкость к атакам, направленным на их математический базис. Поэтому в последнее время значительно возрос интерес к атакам, направленным на конкретные реализации этих алгоритмов. Одной из наиболее эффективных и, в следствие этого, часто рассматриваемых в современной научной литературе атак является так называемая атака с внедрением ошибки (fault injection attack). Суть ее состоит в том, что если злоумышленнику удастся вызвать сбой в процессе выполнения криптографических преобразований в системе шифрования и воспользоваться результатами ее работы, то это значительно облегчит ему взлом и позволит получить секретный ключ.

Впервые теоретическая возможность и перспективы использования подобной атаки были рассмотрены в работах Д. Боне, Р. А. де Милло и Р. Дж. Липтона, а позже появились практические реализации метода для таких известных и распространенных симметричных алгоритмов шифрования как AES и RC5.

Большинство решений, представленных в отечественных и зарубежных публикациях, сосредоточено на решении проблемы возникновения ошибок для конкретных алгоритмов шифрования или их отдельных преобразований в различных специфических условиях, тогда как существует необходимость в разработке общей методологии и обобщенной теории решения описанной проблемы.

Выполнен анализ структур множества наиболее часто используемых алгоритмов шифрования и рассмотрены операции, которые используются в преобразованиях этих алгоритмов. Все современные алгоритмы шифрования используют определенный набор операций, который включает в себя практически все элементарные логические и арифметические функции.

Определены наиболее подходящие способы определения ошибок для аппаратных реализаций криптографических операций. Для некоторых операций существует несколько вариантов реализации механизмов обнаружения ошибок функционирования. Выбор конкретного варианта зависит от используемого алгоритма, особенностей аппаратной платформы и размера операндов.